Enabling Security Transformation

Jeanette Manfra
Director, Risk & Compliance, Google Cloud
Five considerations for your transformation

- What a digital transformation means for security and risk functions
- Understanding the key roles and responsibilities
- Security organisation and operational models
- Antipatterns and other things to watch out for
- Security culture
The Impact of Digital Transformation
Digital transformation **drivers and outcomes**

**Speed of IT Delivery**
The opportunity to enable development teams to deliver IT at pace and innovate quickly. The evolution of application security.

**Infrastructure as Code**
Dynamic management of infrastructure. The opportunity to bake software-grade control into infrastructure and policy management.

**Perimeter is Challenged**
A hard outer shell doesn’t help in the way that it used to. AuthN, AuthZ and configuration management / verification are key.

---

**Continuous Assurance of Controls for ‘Security in the Cloud’**

**Clarity of Shared Responsibilities and Oversight of ‘Security of the Cloud’**
Roles and Responsibilities
## Key roles and responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy &amp; Risk Management</strong></td>
<td>Assesses the policy and risk frameworks for suitability with cloud security models</td>
</tr>
<tr>
<td><strong>Security Architecture &amp; Design</strong></td>
<td>Defines the approach to ‘security in the cloud’</td>
</tr>
<tr>
<td><strong>Security Testing</strong></td>
<td>Performs security-focused testing pre-release</td>
</tr>
<tr>
<td><strong>Security Operations</strong></td>
<td>Detects and responds to events, incidents, and threat intelligence</td>
</tr>
<tr>
<td><strong>Security Assurance</strong></td>
<td>Verifies that architectures are being adhered to and that controls are operational</td>
</tr>
<tr>
<td><strong>Security Engineering</strong></td>
<td>Develops commonly used security toolkits, frameworks and libraries</td>
</tr>
<tr>
<td><strong>Infrastructure Engineering</strong></td>
<td>Engineers and operates the cloud infrastructure and supporting services</td>
</tr>
<tr>
<td><strong>Application Development</strong></td>
<td>Develops applications that are deployed in the cloud infrastructure</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Policy &amp; Risk Management</td>
<td>Refactors policies and standards to ensure focus on the right controls</td>
</tr>
<tr>
<td>Security Architecture &amp; Design</td>
<td>Enables more nimble use of cloud with blueprints that incorporate guardrails</td>
</tr>
<tr>
<td>Security Testing</td>
<td>Moves closer to the development team, tighter integration with SDLC</td>
</tr>
<tr>
<td>Security Operations</td>
<td>Extends monitoring to the cloud, uses the cloud to monitor</td>
</tr>
<tr>
<td>Security Assurance</td>
<td>Becomes configuration and data-centric; focuses on ‘continuous control monitoring’</td>
</tr>
<tr>
<td>Security Engineering</td>
<td>Develops cloud native security toolkits, and defines security policy in code</td>
</tr>
<tr>
<td>Infrastructure Engineering</td>
<td>Adopts software development methodologies to manage infrastructure</td>
</tr>
<tr>
<td>Application Development</td>
<td>Moves from waterfall to agile and automated software delivery</td>
</tr>
</tbody>
</table>
Operating Models
Model 1: Centralised Security

Central Security Function

- Policy & Risk Management
- Security Architecture & Design
- Security Testing
- Security Operations
- Security Assurance
- Security Engineering

Pros: consistency, control, cost efficiency for smaller organisations
Cons: impedes speed of IT delivery, absolution of security responsibilities
Model 2: Federated Security

Central Security Function

- Policy & Risk Management
- Security Operations

Pros: security tightly integrated with SDLC, speed and agility, “just enough” security
Cons: lack of independent assurance, bespoke “roll your own” security solutions

Pros: security tightly integrated with SDLC, speed and agility, “just enough” security
Cons: lack of independent assurance, bespoke “roll your own” security solutions
Model 3: Hybrid Security

Central Security Function

- Policy & Risk Management
- Security Architecture & Design
- Security Testing
- Security Operations
- Security Assurance
- Security Engineering

Pros: common methods & tooling, complex functions get the right support, independent assurance
Cons: requires good communication and collaboration to maintain common vision

Infrastructure Engineering
- Security Coordinator (dedicated or assigned role)

Application Development
- Security Coordinator (dedicated or assigned role)
- Security Architecture & Design
- Security Testing
- Security Engineering

Security is organised and operated according to the needs of the IT team, and the security complexity of their product.
Antipatterns!
Cloud Security Organisational Antipatterns


2. Assuming that existing control implementations are effective (or even necessary) in the cloud. Consider reviewing the control objectives you have first.

3. Assuming that existing security administration and change processes will work for the cloud (particularly centralised processes). They could hamper cloud-enabled teams, who may in turn find workarounds.

4. Relying on historical approaches to assuring compliance with policies and standards. Adopt a data-driven approach to achieve the scale and velocity needed for continuous controls monitoring.
Attributes of a Healthy Security Culture

1. Culture of Security by Default. Security is an assumed part of all stages of IT.
2. Culture of Review. Open, transparent, constructive peer reviews are the norm.
3. Culture of Awareness. Pervasive and innovative (and fun!) education.
5. Culture of Inevitably. Open discussion of failure scenarios and planning to respond.
6. Culture of Sustainability. Balancing work between operating and improving.
Best practices for your cloud security transformation

Take a risk-informed **NOT** a risk-avoidance approach

Embrace zero trust and **forget** the perimeter

**Prioritize** automation to reduce manual workload on security teams

Plan for the training and **reskilling** of your existing security workforce

**Demand** a strong partnership with cloud providers based on shared understanding of risk and security objectives
More information via Google SRE